March 17, 2009

Smart Phone Tool Specification

Public Draft 1 of Version 1.0

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Abstract

As mobile devices proliferate, incorporating a host of integrated features and capabilities, their use can be seen everywhere in our world today. Mobile communication devices contain a wealth of sensitive and non-sensitive information. In the investigative community their use is not restricted to data recovery alone as in criminal cases, but also civil disputes and proceedings, and their aggregate use in research and criminal incident recreation continues to increase. Due to the exploding rate of growth in the production of new mobile devices appearing on the market each year is reason alone to pay attention to test measurement means and methods. The methods a tool uses to capture, process, and report data must incorporate a broad range of extensive capabilities to meet the demand as a robust data acquisition tool. In general, a forensic examination conducted on a mobile device is only a small subset of the larger field of digital forensics. Consequentially, tools possessing an exhaustive array of capabilities to acquire data from these portable mobile devices are relatively few in number.

This paper defines requirements for mobile device applications capable of acquiring data from smart phones operating over a Global System for Mobile communication (GSM) network and a Code Division Multiple Access (CDMA) network, and test methods used to determine whether a specific tool meets the requirements for producing measurable results.[•] Test requirements are statements used to derive test cases that define expectations of a tool or application. Test cases describe the combination of test parameters required to test each assertion. Test assertions are described as general statements or conditions that can be checked after a test is executed. Each assertion appears in one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results. The associated assertions and test cases are defined in the test plan document entitled: Smart Phone Acquisition Tool Test Assertions and Test Plan.

Comments and feedback are welcome; revisions of this document are available for download at: http://www.cftt.nist.gov/mobile_devices.htm.

[•] NIST does not endorse nor recommend products or trade names identified in this paper. All products used in this paper are mentioned for use in research and testing by NIST.

TABLE OF CONTENTS

1. Introduction 1
2. Purpose 1
3. Scope 2
4. Definitions 2
5. Background 4
5.1 Smart Phone Characteristics – Internal Memory 4
5.2 SIM Characteristics 4
5.3 Digital Evidence 4
5.4 Test Methodology 5
6. Requirements 5
6.1 Requirements for Core Features 5
6.2 Requirements for Optional Features 6
6.2.1 SIM Acquisition 6
6.2.2 Presentation 6
6.2.3 Protection 6
6.2.4 Physical Acquisition 7
6.2.5 Log Files 7
6.2.6 Non-ASCII Characters 7
6.2.7 PIN Attempts 7
6.2.8 PUK Attempts 7
6.2.9 Stand-alone Acquisition 7
6.2.10 Hashing 7

1. Introduction

The need to ensure the reliability of mobile device forensic tools intensifies, as the embedded intelligence and ever-increasing storage capabilities of mobile devices expand. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools. This is accomplished by the development of both specific and common rules that govern tool specifications. We adhere to a disciplined testing procedure, established test criteria, test sets, and test hardware requirements, that result in providing necessary feedback information to toolmakers so they can improve their tool's effectiveness; end users benefit in that they gain vital information making them more informed about choices for acquiring and using computer forensic tools, and lastly, we impart knowledge to interested parties by increasing their understanding of a specific tool's capability. Our approach for testing computer forensic tools is based on established well-recognized international methodologies for conformance testing and quality testing. For more information on mobile device forensic methodology please visit us at: http://www.cftt.nist.gov/.

The Computer Forensic Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

The central requirement for a sound forensic examination of digital evidence is that the original evidence must not be modified (i.e., the examination or capture of digital data from a mobile device and associated media must be performed without altering the device or media content). In the event that data acquisition is not possible using current technology to access information without configuration changes to the device (e.g., loading a driver), the procedure must be documented.

2. Purpose

This document defines requirements for mobile device forensic tools used in digital forensics capable of acquiring internal memory from GSM smart phones and associated media (i.e., Subscriber Identity Modules [SIM]), the internal memory of CDMA smart phones and test methods used to determine whether a specific tool meets the requirements.

The requirements are used to derive assertions. The assertions are described as general statements of conditions that can be checked after a test is executed. Each assertion generates one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

3. Scope

The scope of this specification is limited to software tools capable of acquiring the internal memory of smart phones (i.e., GSM, CDMA) and associated media (i.e., SIM). Smart phones often have companion PC-based software that provides users the ability to synchronize data between the device and a personal computer. Requirements are specific to data stored in the internal memory of the smart phone. The specifications are general and capable of being adapted to other types of mobile device forensic software.

4. Definitions

This glossary was added to provide context in the absence of definitions recognized by the computer forensics community.

Associated data: Multi-media data (i.e., graphic, audio, video) that are attached and delivered via a multi-messaging service (MMS) message.

Acquisition File: A snapshot of data contained within the internal memory of a target device or associated media (i.e. SIM).

Case File: A file generated by a forensic tool that contains the data acquired from a mobile device or associated media and case-related information (e.g., case number, property/evidence number, agency, examiner name, contact information, etc.) provided by the examiner.

CDMA: Code Division Multiple Access describes a communication channel access method that employs spread-spectrum technology and a special coding scheme.

Cellular phone: A device whose major function is primarily handling incoming/outgoing phone calls with limited task management applications.

CFT: Cellular Forensic Tool.

CHV: Card Holder Verification.

Electronic Serial Number (ESN): ESNs were issued until 2005, which uniquely identified CDMA phones. An ESN number consist of a 32-bit alpha-numeric string that allowed a maximum of 4 billion unique numbers.

Enhanced Message Service (EMS): Text messages over 160 characters or messages that contain either Unicode characters or a 16x16, 32x32 black and white image.

Flash memory: Non-volatile memory that retains data after the power is removed.

GSM: Global System for Mobile communications is an open, digital cellular technology for transmitting mobile voice and data services.

Hard reset: Rebooting the smart phone in a manner that returns the device back to the initial factory install state, potentially erasing all user data (e.g., contacts, tasks, calendar entries).

Hashing: A mathematical algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the hash value, such that any change to the data will almost certainly change the hash value.

Human-readable format: Acquired data shown in a human language rather than binary data.

IM: Internal Memory.

Logical acquisition: Implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition).

Mobile Equipment Identity (MEID): An ID number that is globally unique for CDMA mobile phones, identifying the device to the network and can be used to flag lost or stolen devices.

Mobile Subscriber International Subscriber Directory Number (MSISDN): The MSISDN conveys the telephone number assigned to the subscriber for receiving calls on the phone.

Multimedia Messaging Service (MMS) message: Provides users with the ability to send text messages containing multimedia objects (i.e., graphic, audio, video).

PIN: A 4 to 8 digit Personal Identification Number that is used to secure mobile devices from unauthorized access.

Preview pane: Section of the Graphical User Interface (GUI) that provides a snapshot of the acquired data.

Physical acquisition: A bit-by-bit copy of the mobile device internal memory.

Personal Information Management (PIM) data: Data that contains personal information such as: calendar entries, to-do lists, memos, reminders, etc.

PUK: A Personal Unblocking Key used to regain access to a locked mobile device whose PIN attempts have been exhausted.

Short Message Service (SMS): A service used for sending text messages (up to 160 characters) to mobile devices.

Smart phone: A full-featured mobile phone that provides users with personal computer like functionality by incorporating PIM applications, enhanced Internet connectivity and email operating over an Operating System supported by accelerated processing and larger storage capacity compared with present cellular phones.

Stand-alone data: Data (e.g., graphic, audio, video) that is not associated with or has not been transferred to the device via email or MMS message.

Subscriber Identity Module (SIM): A smart card that contains essential subscriber information and additional data providing network connectivity to mobile equipment operating over a GSM network.

Supported Data Objects: Data objects (e.g., subscriber information, PIM data, SMS messages, stand-alone data, MMS messages and associated data) that the cellular forensic tool has the ability to acquire according to the cellular forensic tool documentation.

User data: Data populated onto the device using applications provided by the device.

5. Background

5.1 Smart Phone Characteristics – Internal Memory

Smart phones provide users with enhanced PIM applications, the ability to send and receive email, connect to the Internet, and the ability to place and receive calls, maintain data in two regions (i.e., Flash Read Only Memory (ROM) and Random Access Memory (RAM). Typically, operating system (OS) and pre-loaded applications supplied by the manufacturer are stored in flash ROM providing protection against erasure during the event of a hard reset or battery exhaustion. RAM is generally divided into two regions, program memory and an object store. Program memory (used for program execution, loading drivers, and storage for processing information) is cleared much like RAM on a personal computer. The object store retains data during active and quiescent states, but risks data loss in the event of battery exhaustion or a hard reset. Manufacturers may provide users of smart devices with an allocated safe-store folder, providing the ability to protect pre-defined data against erasure in the event of a hard reset or battery depletion. Although data present on smart phones may be stored in a proprietary format, forensic tools tailored for smart phone acquisition should minimally be able to perform a logical acquisition for supported devices and provide a report of the data present in the internal memory. Tools that possess a low-level understanding of the proprietary data format for a specific device may provide examiners with the ability to perform a physical acquisition and generate reports in a meaningful (i.e., human-readable) format.

5.2 SIM Characteristics

Due to the GSM 11.11[1] standard, mobile device forensic tools designed to extract data from a SIM either internally or with an external SIM reader, should be able to properly acquire, decode, and present data in a human-readable format. An abundance of information is stored on the SIM such as Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), Short Message Service (SMS) messages, subscriber information (e.g., IMSI), and location information (i.e., Location Information [LOCI], General Packet Radio Service Location [GPRSLOCI]).

5.3 Digital Evidence

The amount and richness of data contained on smart phones varies based upon the manufacturer and OS. Pre-loaded applications and the ability to install customized applications provide users with endless solutions. However, there is a core set of data that computer forensic tools can recover that remains somewhat consistent on all smart phones. Tools should have the ability to recover the following data objects stored in the device's internal handset memory and associated media:

- International Mobile Equipment Identifier (IMEI) – GSM device memory
- Mobile Equipment Identifier (MEID) / Electronic Serial Number (ESN) – CDMA device memory
- Service Provider Name (SPN) – SIM memory
- Integrated Circuit Card Identifier (ICCID) – SIM memory
- International Mobile Subscriber Identity (IMSI) – SIM memory
- Mobile Subscriber International ISDN Number (MSISDN) – SIM memory

[1] http://www.ttfn.net/techno/smartcards/gsm11-11.pdf

- Personal Information Management (PIM) data – (e.g., Address book, Calendar entries, to-do list, Tasks, Memos) – device memory
- Abbreviated Dialing Numbers (ADNs) – SIM memory
- Application Data – (e.g., word documents, spreadsheet data, presentation data, etc.) – device memory
- Internet Data – (e.g., bookmarks, visited sites, cached URLs) – device memory
- Call logs – Incoming and outgoing calls – device memory
- Last Numbers Dialed (LND) – SIM memory
- Text messages (SMS, EMS) – device memory, SIM memory
- Multi-media Messages (MMS)/email – and associated data (i.e., audio, graphics, video) – device memory
- File storage – Stand-alone files such as audio, graphic and video – device memory

5.4 Test Methodology

To provide repeatable test results, the following test methodology is strictly followed. Each forensic application under evaluation is installed on a dedicated (i.e., no other forensic applications are installed) host computer operating with the required platform as specified by the application. The internal memory of the source device and associated media (i.e., SIM) is populated with a pre-defined dataset. Data population techniques and procedures are outlined in the Smart Phone Tool Setup and Test Procedures document. Source devices are stored in a protected state subsequent to initial data population, thus eliminating the possibility of data modification due to network connectivity. Each succeeding test entails recreating the host-testing environment for each specific tool tested.

The following data objects will be used in populating the internal memory of the smart phone: address book, PIM data, application data, Internet data, call logs, text messages (SMS, EMS), MMS messages/email with attachments (i.e., audio, graphic, video) and stand-alone data files (i.e., audio, graphic, video). The following data objects will be used for populating the SIM: Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), Short Messaging Service (SMS) messages – (marked as Read, Unread and Deleted), EMS messages, and location (LOCI) information.

6. Requirements

The requirements are in two sections: 6.1 and 6.2. Section 6.1 lists requirements (i.e., Cellular Forensic Tool-Core Requirement-01 [CFT-CR-01] through CFT-CR-05 that all acquisition tools shall meet. Section 6.2 lists requirements (i.e., Cellular Forensic Tool-Requirement Optional-01 [CFT-RO-01] through CFT-RO-16 that the tool shall meet on the condition that specified features or options are offered by the tool.

6.1 Requirements for Core Features

The following core requirements shall be met by all mobile device forensic tools capable of acquiring internal smart phone memory.

CFT-CR-01 A cellular forensic tool shall have the ability to recognize supported devices via the vendor supported interfaces (e.g., cable, Bluetooth, Infrared).

CFT-CR-02 A cellular forensic tool shall have the ability to identify non-supported devices.

CFT-CR-03 A cellular forensic tool shall have the ability to notify the user of connectivity errors between the device and application during acquisition.

CFT-CR-04 A cellular forensic tool shall have the ability to provide the user with either a preview pane or generated report view of data acquired.

CFT-CR-05 A cellular forensic tool shall have the ability to logically acquire all application supported data objects present in internal memory without modification.

6.2 Requirements for Optional Features

The following requirements define optional tool features. If a tool provides the capability defined, the tool is tested for conformance to these requirements. If the tool does not provide the capability defined, the requirement does not apply.

The following optional features are identified:

- SIM acquisition
- Presentation
- Protection
- Physical acquisition
- Log file creation
- Non-ASCII character support
- PIN/PUK input
- Stand-alone acquisition
- Hashing

6.2.1 SIM Acquisition

CFT-RO-01 A cellular forensic tool shall have the ability to recognize supported SIMs via the vendor supported interface (e.g., PC/SC reader, proprietary reader, internal).

CFT-RO-02 A cellular forensic tool shall have the ability to identify non-supported SIMs.

CFT-RO-03 A cellular forensic tool shall have the ability to notify the user of connectivity errors between the SIM reader and application during acquisition.

CFT-RO-04 A cellular forensic tool shall have the ability to provide the user with the opportunity to unlock a password protected SIM before external reader SIM acquisition.

CFT-RO-05 A cellular forensic tool shall have the ability to acquire all application-supported data objects present in the SIM memory without modification.

6.2.2 Presentation

CFT-RO-06 A cellular forensic tool shall have the ability to provide a presentation of acquired data in a human-readable format via a generated report.

CFT-RO-07 A cellular forensic tool shall have the ability to provide a presentation of acquired data in a human-readable format via a preview pane view.

6.2.3 Protection

CFT-RO-08 A cellular forensic tool shall have the ability to protect previously acquired data objects within a saved case file from modification.

6.2.4 Physical Acquisition

CFT-RO-09 A cellular forensic tool shall have the ability to perform a physical acquisition of the device's internal memory without modification for supported devices.

6.2.5 Log Files

CFT-RO-10 A cellular forensic tool shall have the ability to create user-accessible and readable log files documenting the acquisition process.

6.2.6 Non-ASCII Characters

CFT-RO-11 A cellular forensic tool shall have the ability to present data objects containing non-ASCII characters acquired from the internal memory of the device or SIM via the selected interface (i.e., preview pane, generated report). Non-ASCII characters shall be printed in their native representation.

6.2.7 PIN Attempts

CFT-RO-12 A cellular forensic tool shall have the ability to present the remaining number of CHV1/CHV2 PIN unlock attempts.

6.2.8 PUK Attempts

CFT-RO-13 A cellular forensic tool shall have the ability to present the remaining number of PUK unlock attempts.

6.2.9 Stand-alone Acquisition

CFT-RO-14 A cellular forensic tool shall have the ability to acquire internal memory data without modifying data present on the SIM.

6.2.10 Hashing

CFT-RO-15 A cellular forensic tool shall have the ability to compute a hash for individual data objects.

CFT-RO-16 A cellular forensic tool shall have the ability to compute a hash for the overall case file.